FORM PTO-1390 (REV 12-29-99) U S DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE

TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371

ATTORNEY'S DOCKET NUMBER: 82032-0002

U.S. APPLICATION NO (If known, see 37 CFR 1 5): 09/601233

INTERNATIONAL APPLICATION NO.	INTERNATIONAL FILING DATE	PRIORITY DATE CLAIMED
PCT/EP99/09575	07 December 1999 (07.12.99)	08 December 1998 (08.12.98)

TITLE OF INVENTION

SYSTEM FOR PROCESSING AN INFORMATION SIGNAL

APPLICANT(S) FOR DO/EO/US

Andrew Augustine WAJS, Gerard Johan DEKKER

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. X This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. X This express request to begin national examination procedures (35 U.S.C. 371(f)) at any time rather than delay examination until the expiration of the applicable time limit set in 35 U.S.C. 371(b) and PCT Articles 22 and 39(1).
4. ☐ A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date
5. X A copy of the International Application as filed (35 U.S.C. 371(c)(2))
   a. ☐ is transmitted herewith (required only if not transmitted by the International Bureau).
   b. X has been transmitted by the International Bureau.
   c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US).
6. ☐ A translation of the International Application into English (35 U.S.C. 371(c)(2)).
7. ☐ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(c)(3))
   a. ☐ are transmitted herewith (required only if not transmitted by the International Bureau).
   b ☐ have been transmitted by the International Bureau.
   c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
   d. ☐ have not been made and will not be made
8. ☐ A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371 (c)(3)).
9. X An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)).
10. ☐ A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

Items 11. to 16. below concern document(s) or information included:

11. ☐ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
12. X An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
13. X A FIRST preliminary amendment.
    ☐ A SECOND or SUBSEQUENT preliminary amendment.
14. ☐ A substitute specification
15. ☐ A change of power of attorney and/or address letter.
16. X Other items or information:

    -Courtesy copy of the International Application as published with International Search Report.

533 Rec'd PCT/PTO 31 JUL 2000

U.S. APPLICATION NO. (if known, see 37 CFR 1.5)	INTERNATIONAL APPLICATION NO	ATTORNEY'S DOCKET NUMBER
09/601233	PCT/EP99/09575	82032-00002

17. X The following fees are submitted:

BASIC NATIONAL FEE (37 CFR 1.492 (a) (1) - (5):

Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO and International Search Report not prepared by the EPO or JPO **$970.00**

International preliminary examination fee (37 CFR 1.482) not paid to USPTO but International Search Report prepartd by the EPO or JPO **$840.00**

International preliminary examination fee (37 CFR 1.482) not paid to USPTO but international search fee (37 CFR 1.445(a)(2)) paid to USPTO **$690.00**

International preliminary examination fee paid to USPTO (37 CFR 1.482) but all claims did not satisfy Provisions of PCT Article 33(1)-(4) **$670.00**

International preliminary examination fee paid to USPTO (37 CFR 1.482) and all claims satisfied provisions of PCT Article 33(1)-(4) **$96.00**

	CALCULATIONS PTO USE ONLY	
ENTER APPROPRIATE BASIC FEE AMOUNT =	$840.00	
Surcharge of **$130.00** for furnishing the oath or declaration later than ☐ 20 X 30 months from the earliest claimed priority date (37 CFR 1.492(e)).	$	

CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE		
Total claims	31-20 =	11	X $18.00	$198.00	
Independent claims	3- 3 =		X $78.00	$	
MULTIPLE DEPENDENT CLAIM(S) (if applicable)			+$260.00	$	
TOTAL OF ABOVE CALCULATIONS =				$1,038.00	
Reduction of 1/2 for filing by small entity, if applicable. A Small Entity Statement must also be filed (Note 37 CFR 1.9, 1.27, 1.28).					
SUBTOTAL =				$1,038.00	
Processing fee of **$130.00** for furnishing the English translation later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492(f)). +					
TOTAL NATIONAL FEE =				$1,038.00	
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). **$40.00** per property +				$ 40.00	
TOTAL FEES ENCLOSED =				$1,078.00	
				Amount to be refunded:	$
				charged:	$

a. X A check in the amount of $1,078.00 to cover the above fees is enclosed.

b. ☐ Please charge my Deposit Account No. _____ in the amount of $_____ to cover the above fees. A duplicate copy of this sheet is enclosed.

c. X The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 50-1349. A duplicate copy of this sheet is enclosed.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:
HOGAN & HARTSON LLP
Celine Jimenez Crowson
555-13th Street, N.W., 7W
Washington, D.C. 20004
(202) 637-5703

SIGNATURE

CELINE JIMENEZ CROWSON
NAME

40,357
REGISTRATION NUMBER

09/601233

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

533 Rec'd PCT/PTO 31 JUL 2000

In re Application of:	)	
Andrew A. WAJS et al.	)	371 of International Application
Serial No.: **not yet assigned**	)	IA #: **PCT/EP99/09575**
Filed: **even date herewith**	)	IA Date: **07 December 99**
Title: **SYSTEM FOR PROCESSING AN INFORMATION SIGNAL**	)	ATTY DKT NO.: **82032-00002**

PRELIMINARY AMENDMENT

Commisioner of Patents and Trademarks
Washington, D.C.

Sir:

Prior to calculation of the filing fee and examination on the merits, please amend the above-identified application as follows.

IN THE CLAIMS:

Claim 5, line 1, delete "or 4".

Claim 6, line 1, delete "or 4".

Claim 7, line 1, delete "or 6".

Claim 9, line 1, delete "or 8".

Claim 10, line 1, delete "8 or 9,"

Claim 11, line 1, change "any one of the claim 3-10" to --claim 3--.

Claim 18, line 1, delete "or 17".

Claim 19, line 1, change "any one of claim 15-18" to --claim 15--.

Claim 20, line 1, change "any one of claims 14-19" to --claim 14--.

Claim 22, line 1, change "any one of claims 14-21" to --claim 14--.

Claim 24, line 1, delete "or 23".

Claim 25, line 1, change "any one of claims 14-24" to --claim 14--.

Claim 27, line 1, delete "according to any one of claims 19-25".

HOGAN & HARTSON
L.L.P.
COLUMBIA SQUARE
555 THIRTEENTH STREET NW
WASHINGTON DC 20004-1109
(202) 637-5600

REMARKS

The above amendments are being made to delete multiple dependencies in the claims and do not add to or depart from the original disclosure or constitute prohibited new matter.

Respectfully submitted,

Celine ~~Jimenez~~ Crowson
Attorney for Applicant
Registration No. 40,357
Hogan & Hartson, LLP
555 13th Street, N.W., Suite 701-W
Washington, D.C. 20004
PH: 202-637-5600

HOGAN & HARTSON
L.L.P.
COLUMBIA SQUARE
555 THIRTEENTH STREET NW
WASHINGTON DC 20004-1109
(202) 637-5600

System for processing an information signal

The invention relates to a system for processing an information signal, comprising a system for scrambling the information signal and at least one system for descrambling the scrambled information signal. The invention further relates to a system for scrambling an information signal, a system for descrambling a scrambled information signal, and to applications of these systems.

In known systems of this type the clear information signal is compressed and then the compressed information signal is scrambled to protect the information signal against unauthorised copying. For obtaining the clear information signal, the scrambled compressed information signal is first descrambled and thereafter decompressed. However in the available systems wherein the clear information signal is provided by descrambling and decompressing, it is relatively easy for an unauthorised person to copy the descrambled information signal which is still compressed. In this manner a clear compressed copy of the information signal becomes available to an unauthorised person. This is a serious disadvantage of the known systems.

The present invention aims to provide improved systems of the above-mentioned type, wherein protection against copying of the information signal is significantly improved.

According to the invention a system for processing an information signal is provided, comprising a system for scrambling the information signal and at least one system for descrambling the scrambled information signal, said scrambling system comprising means for analysing the entropy distribution of the information signal, means for scrambling the information signal in dependence on the entropy distribution of the information signal to provide a scrambled information signal having an entropy distribution corresponding with the entropy distribution of the information signal

and means for compressing the scrambled information signal, said descrambling system comprising means for decompressing the compressed scrambled information signal, means for descrambling the scrambled information signal to provide the information signal.

The invention is based on the insight that it is possible to use existing compressing techniques on a scrambled information signal provided that the entropy distribution of the scrambled information signal is not significantly changed with respect to original information signal. By analysing the information signal to determine the entropy distribution the scrambling can be carried out such that the entropy distribution is hardly changed. Although the information in the scrambled signal will generally not be hidden completely, the quality of the scrambled signal will be such that it cannot be used without descrambling.

The invention further provides scrambling and descrambling systems operating according to the same principle, and applications of these systems.

The invention will be further explained by reference to the drawings in which some embodiments of the different systems of the invention are schematically shown.

Fig. 1A and 1B show a block diagram of a first embodiment of the system for processing an information signal according to the invention.

Fig. 2A and 2B show a block diagram of an embodiment of the invention used for scrambling and descrambling an audio signal.

Fig. 3 shows an application of the system of the invention for audio distribution over the Internet.

Fig. 4 shows an application of the system of the invention for information broadcast over the Internet.

Fig. 5 schematically shows an application of the invention in DVD-players.

Referring to fig. 1A and 1B there is shown a system for processing an information signal, which system comprises a system 1 for scrambling the information signal (Fig. 1A) and at least one system 2 for descrambling the scrambled in-

formation signal (Fig. 1B). Although only one descrambling system is shown in Fig. 1B the system may include a number of such descrambling systems. The scrambling system 1 comprises an analyser or means for analysing 3 receiving the information signal to be compressed from an input 4. The analyser 3 analyses the information signal to determine the entropy distribution of this signal. In case of an audio signal for example, the analyser 3 may include a number of narrow band filters as will be described hereinafter. The scrambling system 1 further comprises generating means 5 for generating a noise signal. In the embodiment described this generating means is made as a white noise generator, for example a pseudo random signal generator. This noise generator 5 receives a key from a control unit 6. The control unit 6 receives information on the entropy distribution from the analyser 3 and provides scrambling control information to a processor 7 which receives the noise output signal from the noise generator 5. The scrambling control information controls the processor 7 in such a manner that the processor 7 provides a noise signal on an output 8 having an entropy distribution corresponding with the entropy distribution of the information signal received on the input 4. The information signal is scrambled by combining this information signal with the processed noise signal on the output 8 in a scrambler 9. The scrambler 9 may include a simple adding or subtracting operation.

The scrambler 9 provides a scrambled information signal on an output 10 to a compressor 11. The compressor 11 may operate according to any suitable compression algorithm and provides a compressed scrambled information signal on an output 12. The scrambled compressed information signal can be transferred to the descrambling system 2 in any known manner, for example over the Internet, by broadcasting or stored on a suitable medium, such as a tape or CD.

The scrambling system 1 described shows the advantage that the scrambled output signal of the scrambler 9 has an entropy distribution corresponding with the entropy distribution of the information signal received on the input 4.

In this manner the entropy distribution of the information signal is not changed by the scrambling operation so that any compression algorithm which is able to compress the clear information signal will be able to compress the scrambled information signal with substantially the same effectiveness.

The control unit 6 provides a key and entitlement file on an output 13, which file can be scrambled using a suitable scrambling algorithm, known per se. For scrambling the key and entitlement file, a private key of the descrambling system 2 is preferably used. The key and entitlement file can be transferred to the descrambling system 2 in any suitable manner.

The descrambling system 2 comprises a decompressor 14 receiving the compressed scrambled information signal from an input 15 of the descrambling system 2. The decompressor 14 may operate according to any suitable decompression algorithm. Within one system the same compression / decompression algorithm will be used. The decompressed output from the decompressor 14 is provided to a descrambler 16 which provides the clear information signal on an output 17 of the descrambling system 2. The descrambler 16 receives a descrambling signal on an input 18 and for providing this descrambling signal, the descrambling system 2 is provided with the following devices.

As shown in fig. 1B, a control unit 19 is provided receiving the key and entitlement file and scrambling control information from the scrambling system 1. The key and entitlement file are forwarded to a secure device 20 which is tamper proof and can be a smart card for example. The secure device 20 comprises a noise generator 21 generating white noise. The noise generator 21 is made as a pseudo random noise generator corresponding to the pseudo random signal generator 5. The key received from the scrambling system 1 is used as a seed for this noise generator 21. In this manner the output noise signal of the generator 21 corresponds with the output noise signal of the generator 5. The output noise signal of the generator 21 is provided to a

processor 22 which is controlled by the scrambling control information received from the scrambling system 1 to process the noise output signal to provide a processed noise signal on an output 23 corresponding to the processed noise output signal of the processor 7 and therefore having an entropy distribution corresponding with the entropy distribution of the clear information signal.

In the preferred embodiment shown in fig. 1B, the processed noise signal on the output 23 is further processed in an equaliser 24 to compensate for any alterations in the scrambled information caused by the compression and decompression operations. Any alterations by the compression and decompression operations will also affect the scrambling signal included in the scrambled information signal, so that the processed noise signal provided by the processor 22 should be compensated for these alterations. In this manner the descrambling operation will be improved. The thus obtained descrambling signal is combined with the decompressed output from the decompressor 14 in the descrambler 16 which provides the clear information signal.

Although in the embodiments described above and hereinafter, respectively, a compressor 11 and decompressor 14 are included in the scrambling and descrambling system, respectively, it is noted that compressing and decompressing can be carried out in separate devices or steps.

The descrambling system 2 described will generally be part of a consumer electronic device or a PC. The descrambling system 2 shows the advantage that only a decompressed clear signal is available in the consumer device or PC. Unauthorised distribution of compressed files would require recompression before such files can be stored or redistributed across a network, for example. A major advantage is further that the noise generator 21 is included in the secure device 20 and that a high bandwidth noise signal is provided as an output signal. This makes redistribution of this noise signal extremely difficult in comparison to redistribution of the key used as a seed for the noise generator 21.

According to a preferred embodiment, protection against unauthorised copying of the information signal can be further increased by providing the secure device 20 with a processor 25 adapted to add a watermark signal to the output of the noise generator 21. The watermark signal may be obtained by combining a pseudo random sequence with a identification sequence. Any parts necessary to generate those sequences are deemed to be comprised in the processor 25. The watermark signal will be part of the descrambling signal provided to the descrambler 16 so that this watermark signal will be part of the clear information signal on the output 17. If the output signal would be recompressed, and this recompressed signal would be used for unauthorised copying or redistribution, the secure device 20 used for this purpose can be traced by means of the watermark signal. Regarding the manner in which a watermark signal can be added, reference is made to a co-pending application of the same applicant which is incorporated herein by reference.

A further protection against copying can be obtained by using the processor 25 of the secure device 20 to add a compression hindering signal to the noise output of the noise generator 21. This compression hindering signal will then be part of the descrambling signal used by the descrambler 16 and will be inserted in this manner into the information signal on the output 17. The compression hindering signal for example inserts noise into the information signal which will not affect the quality of the information signal. It will however significantly affect the compression algorithms to effectively compress the information signal.

In case of digital information signals a further protection against unauthorized copying could be added as follows. The descrambling system 2 can be provided with means for converting the decompressed but still scrambled signal from digital into analogue. Further, means for converting the descrambling signal from digital into analogue are provided. The thus obtained analogue scrambled signal and descrambling siganl are combined in the descrambler 16 to obtain a clear analogue information signal.

Figs. 2A and 2B show an application of the system of the invention as generally described above for scrambling and descrambling audio signals. Fig. 2A shows the scrambling system which in the embodiment shown is adapted to operate on digital audio signals. However, the system can be implemented in the same manner for analogue audio signals. The scrambling system 1 comprises a plurality n of narrow band filters 26 corresponding to the analyser 3 of the system shown in fig. 1. The narrow band filters 26 each provide information on the signal strength in the respective bands to the control unit 6. The noise generator 5 provides an output signal to a further plurality n of narrow band filters 27, wherein the control unit 6 enables only those filters corresponding to the narrow band filters 26, the outputs of which indicated a signal strength in the audio signal. The gain of each of the band filters 27 is adjusted by the control unit such that the noise output signal strength corresponds with the signal strength in the corresponding band of the audio signal. The outputs of the band filters 27 are summed to provide the scrambling signal as shown by block 28. The scrambling signal is combined with the audio signal in scrambler 9 and the output of scrambler 9 is compressed by compressor 11.

The descrambling system 2 is only partially shown in fig. 2B and comprises a plurality of narrow band filters 29 corresponding to the narrow band filters 27. The noise generator 21 corresponds with the noise generator 5 of the scrambling system and is seeded by the key received from the scrambling system 1. The control unit 19 receives the scrambling control information from the control unit 6 and enables the same filters 29 in the descrambling system 2 as the filters 27 enabled by the control unit 6. The gain of the enabled filters 29 is adjusted accordingly. In this manner the descrambling signal is made by combining the outputs of the filters 29 as indicated by the block 30. The descrambling system 2 for audio signals further fully corresponds with the system shown in fig. 1.

The system shown in fig. 1 can also be used in case

of still images or video signals. In case of still images, the JPEG compression algorithm can be used for example. According to this algorithm an image is divided into blocks of 8x8 pixels . A discrete cosine transform (DCT) is performed on each block. The DCT results in a set of coefficients that are completely orthogonal to each other. The analyser 3 can be adapted to analyse the entropy distribution of DCT sets of coefficients. Further the generator 5 is adapted such that noise is generated in a two-dimensional space and the information provided by the analyser 3 is used to adjust a set of filters to obtain noise having a signal strength corresponding to the significant coefficients in the DCT sets of coefficients. Thereafter the thus obtained scrambling signal is combined with the DCT sets of coefficients, where after the JPEG algorithm can still be used to compress the scrambled signal. The descrambling system operates in a corresponding manner to descramble and decompress the compressed scrambled signal.

In typical implementations of video encoding a still image is utilised as a base. A reference frame is coded using a still image compression scheme, for example the I-frame in the well-known MPEG2 compression algorithm. Scrambling and descrambling of this reference frame occurs in the same manner as described above for a still image. Successive frames are compressed using the previous frame as a reference frame. In the MPEG2 compression algorithm, blocks of the next frame are compared with the reference frame and any part of the reference frame that provides the best match is then used as the reference block. The difference is then coded. A vector is also defined which indicates the position of the reference block with respect to the block being coded. The differences between the two frames are computed and a DCT is performed on the differences and the DCT coefficients are compressed.

According to the invention noise can be added to all or a plurality of blocks in a first or reference frame and this noise needs to be propagated into future frames such that the difference coding remains intact. This means

that at the descrambling system side noise used as descrambling signal needs to be reused as descrambling signal for future blocks. Further scrambling and descrambling can be performed on the next blocks by adding noise to the difference DCT information, wherein as in the described examples the noise added must have the same entropy ditribution as the difference DCT information.

It will be understood that the JPEG and MPEG algorithms and DCT are mentioned as examples only, and should not be explained as limitinhg the invention to such examples.

It is noted that the scrambling control information provided by the control unit 6 can be transfered as a separate file to the descrambling system 2. As a preferred alternative the scrambling control information can be included into the information signal as a type of header or the like, wherein the scrambling control information is modulated to bring this signal in the same frequency band as the information signal.

In the above described embodiments an equaliser 24 is used to compensate for the effects of the compression and decompression. This means that this equaliser actually replicates the transfer function for the process that the information signal undergoes. Depending on the circumstances it can be complicated to determine the transfer function by measuring the impulse response of this process. In the described system of the invention this problem is solved by including an impulse in the beginning of the information signal. The impulse is not scrambled and undergoes the same compression and decompression steps as the information signal. The control unit 19 uses the thus obtained impulse response for the compression and decompression to model the transfer function provided by the equaliser 24. As an alternative a sequence of sine waves covering the frequency bands of interest can be included in the information signal. Again the control unit 19 can measure the attenuation and phase shift of the sine waves received to determine the impulse response of the system.

These examples show that by adding a known signal to the information signal the control unit 19 can measure the impulse response and can adjust the equaliser 24 such that the equaliser replicates the transfer function so that the regenerated scrambling signal in the descrambling system will correspond with the scrambling signal in the scrambling system.

The same technique can be used in case of a system for still images or video signals. In case of still images a black band is added to one side of the image. In one block of the black band an impulse is inserted into the middle of the block. The impulse response can be determined by the control unit by checking the pixels around the pixel corresponding to the impulse inserted. In case of video the same technique as for still images can be used. As an alternative a black frame could be inserted in the sequence of frames. In the middle of this black frame an impulse can be included. The control unit can check the pixels of the black frame around the impulse pixel to determine the impulse response.

By way of example some applications of the system of the invention described are shown in figs. 3,4 and 5.

Fig. 3 shows an application for distribution of audio signals over the Internet. Although at this moment it is already possible to download MP3 audio files from the Internet, the software industry is very reluctant to make available MP3 compressed audio files as in compressed form audio piracy will be trivial and wide spread using the Internet as distribution means. For example someone could legitimately buy an MP3 audio track and distribute the same using E-mail. Even if the compressed audio file is encrypted, pirate software programs to decrypt the content could become available, where after it will be possible to store the clear compressed file for later distribution. These disadvantages of the use MP3 or otherwise compressed audio files can be overcome by using the system of the invention in an application as shown in fig. 3.

It will be understood that although only one con-

sumer PC 31 is shown in fig. 3, any number of PC's can be part of the system, wherein each PC corresponds with one descrambling system 2 of fig. 1. It is assumed that the required decompressing and descrambling software is installed on the PC 31. This software can for example downloaded from the Internet. The consumer using the PC 31 can visit a web site for buying one or more specific audio files. The web site is running on a web server 32 and an audio file server 33, a key and entitlement server 34 and billing system 35 are connected to the web server 32. The web server 32, audio file server 33 and key and entitlement server 34 together provide the scrambling system 1. Although in the embodiment shown in fig. 3, a billing system is used, this is not necessary and the system can also be used in an embodiment without billing system, wherein the consumer is charged in another manner or not charged at all for the downloaded audio files.

When the consumer has made a selection and confirmed the purchase made in any suitable manner, the compressed scrambled audio file and the key and entitlement file are transferred to the PC 31 of the consumer. The audio file is stored on hard disc or any other storage media connected to the PC 31. The entitlement and key file is loaded into the secure device 20 connected to the PC 31. The key and entitlement file is for example encrypted using a key unique to the secure device 20 of the corresponding consumer. The consumer can now replay the audio file as long as the secure device is connected to the PC.

If this consumer would try to distribute the compressed audio file and the key and entitlement file, the audio file will still be scrambled and the key and entitlement file which is specific to the secure device 20 of this specific consumer, will be rejected by any other secure device.

The entitlement provided to the consumer can contain different entitlements, such as for example play once only, play for a limited period of time or a free sample play. Further, a possibility in the entitlement file could

be "anonymous ownership" allowing entitlements and keys to be exchanged between secure devices using secure protocols. The entitlement can be such that only one secure device at a time is allowed to have the entitlement and key. Further it is possible to have an entitlement for group ownership. In this case a consumer could be allowed to play the audio file on a number of audio players owned by this consumer.

If the user of the PC 31 would send a copy of the decompressed audio file to someone else, it will be necessary to recompress the audio file. This will significantly increase the time and effort to make a copy and by using the above-described embodiment of the secure device 20, wherein a watermark signal is added to the descrambling signal, the copy can be traced to the secure device 20 used for descrambling the audio file. Further in case also the compression hindering signal is added to the descrambling signal, the quality of the new copy will be significantly decreased preventing unauthorised distribution.

Fig. 4 shows another application of the system of fig. 1 for broadcast on the Internet. It is noted that the same principle can be used in other types of broadcast networks.

If in the system shown in fig. 4 the PC 31 has tuned on a specific broadcast signal, key and entitlement files are broadcast from the key and entitlement server 34 to the PC 31 and the key and entitlement files are loaded into the secure device 20. The secure device 20 generates the descrambling signal in synchronisation with the compressed and scrambled video files received from the video file server 36, which files can either be provided in real time or be stored on a suitable storage medium.

It is essential that the key which is used to generate the descrambling signal, never appears in the clear. The noise signal provided by the secure device 20 has a large bandwidth, similar to that of the decompressed data, as explained above. Any rebroadcast of the descrambling signal by a pirate can be traced to the corresponding secure device 20 due to the watermark signal added to the descram-

bling signal. In this manner the pirate can be quickly traced and the secure device 20 can be disabled. Rebroadcasting of the video content is neither possible as it is not provided in a clear compressed form. Rebroadcasting would require recompressing the content which will be hindered by adding the compression hindering signal and the rebroadcasted signal can be traced by the watermark signal.

Fig. 5 shows an application of the system of fig. 1 to prevent unauthorised copying of video discs or DVD's. The same principle can be used to prevent unauthorised copying of audio CD's.

In particular with respect to DVD's, software industry is concerned about the protection of the video content. The current mechanisms for copy protection are extremely weak, in particular when a DVD player is coupled with a PC. Basically, all conventional mechanisms rely on the player being tamper resistant to be effective. In practice a DVD player is not tamper resistant. The disadvantage of the current copy protection mechanisms can be overcome by applying the system of the invention, for example in an application as shown in fig. 5.

A DVD player 36 is made such that the player 36 can be coupled with a secure device 20. The DVD player 36 and secure device 20 together provide a descrambling system 2. When a consumer purchases a new DVD, the consumer provides the secure device serial number to the point of sale 37. The point of sale 37 contacts an authorisation centre 38 and this centre 38 generates a key and entitlement file which is transferred to the DVD player and stored in secure device 20. The DVD contains the video information in compressed scrambled form. Once the key and entitlement file is downloaded into the secure device 20, replay of the content is possible as described above. According to the example of fig. 5, the key and entitlement file is downloaded over the Internet. It is of course possible to transfer the key and entitlement file in any suitable manner to the player 36, for example via a modem connection or a floppy disc or the like. The DVD's and key and entitlement files are provided

by using a scrambling system 1 as described above.

It will be clear that the invention provides an improved copy protection which can be used in various applications. Although in the embodiments described and in the drawings separate parts of the systems are mentioned and shown, it will be clear that the systems described can be implemented by means of PC's or other microprocessor based systems in combination with suitable application programs.

The invention is not restricted to the above described embodiments which can be varied in a number of ways within the scope of the following claims.

CLAIMS

1. System for processing an information signal, comprising a system (1) for scrambling the information signal and at least one system (2) for descrambling the scrambled information signal, said scrambling system comprising means (3,6) for analysing the entropy distribution of the information signal, means (5,6,7,9) for scrambling the information signal in dependence on the entropy distribution of the information signal to provide a scrambled information signal having an entropy distribution corresponding with the entropy distribution of the information signal and means (11) for compressing the scrambled information signal, said descrambling system (2) comprising means (14) for decompressing the compressed scrambled information signal, and means (16,19,21,22,24) for descrambling the scrambled information signal to provide the information signal.

2. System according to claim 1, wherein said scrambling means (5,6,7,9) comprises means (5,6,7) for generating a scrambling signal having an entropy distribution corresponding with the entropy distribution of the information signal and means (9) for combining the scrambling and information signals to obtain the scrambled information signal, wherein said descrambling means (16,19,21,22,24) comprises means (19,21,22,24) for regenerating the scrambling signal as a descrambling signal and means (16) for combining the descrambling and scrambled information signals to obtain the information signal.

3. System according to claim 2, wherein said analysing means (3,6) provides scrambling control information and wherein said generating means (5,6,7) generates a noise signal and comprises means (7) for processing said noise signal as controlled by the scrambling control information to obtain the scrambling signal, wherein said scrambling control information is transferred to the descrambling system (2), wherein said regenerating means (19,21,22,24) generates a noise signal and comprises means (22,24) for processing said noise signal as controlled by the scrambling

control information to obtain the descrambling signal.

4. System according to claim 3, wherein the scrambling control information is transferred to the descrambling system as part of the information signal.

5. System according to claim 3 or 4, wherein said generating and regenerating means (5,7;21,22,24) comprises a white noise generator (5,21) and filtering means (7,22) controlled by said scrambling control information to filter the white noise to obtain noise having an entropy distribution corresponding with the entropy distribution of the information signal.

6. System according to claim 3 or 4, wherein said generating and regenerating means (5,7;21,22,24) comprises a narrow band noise signal generator and modulating means for modulating the narrow band noise signal controlled by said scrambling control information to obtain noise having an entropy distribution corresponding with the entropy distribution of the information signal.

7. System according to claim 5 or 6, wherein the noise generator of the generating means (5,7) is a pseudo random noise generator (5) seeded by a key, wherein said regenerating means (21,22,24) comprises a corresponding pseudo random noise generator (21) which is seeded by the same key, wherein means (6) are provided to transfer the key from the scrambling system (1) to the descrambling system (2) in a secure manner.

8. System according to claim 7, wherein the scrambling system (1) comprises means (6) for periodically generating a new key.

9. System according to claim 7 or 8, wherein said scrambling system (1)comprises means (6) for generating entitlement files, wherein said transfer means (6) transfers an entitlement file together with a key to the descrambling system (2).

10. System according to claim 7, 8 or 9, wherein the transfer means (6) insert the key or entitlement file into the information signal to transfer this file as part of the information signal, preferably together with the scram-

bling control information.

11. System according to any one of the claim 3-10, wherein said scrambling system (1) is adapted to insert an impulse response measuring signal into the information signal, wherein the descrambling system (2) is adapted to determine the impulse response of the system by comparing the received impulse response measuring signal with the original impulse response measuring signal, the descrambling system comprising an adjustable equaliser (24) to process the regenerated noise signal, wherein the equaliser is adjusted to model the transfer function of the system.

12. System (1) for scrambling an information signal, comprising means (3,6) for analysing the entropy distribution of the information signal, means (5,6,7,9) for scrambling the information signal in dependence on the entropy distribution of the information signal to provide a scrambled information signal having an entropy distribution corresponding with the entropy distribution of the information signal.

13. System according to claim 12, wherein said analysing means (3,6) provides scrambling control information and wherein said scrambling means (5,6,7,9) comprises generating means (5,6) generating a noise signal and means (7) for processing said noise signal as controlled by the scrambling control information to obtain the scrambling signal, wherein means (6) are provided to transfer the scrambling control information to a descrambling system (2).

14. System (2) for descrambling a scrambled information signal, comprising means (16,19,21,22,24) for descrambling the scrambled information signal to provide the information signal, wherein said descrambling means comprises means (19,21,22,24) for regenerating the scrambling signal as a descrambling signal and means (16) for combining the descrambling and scrambled information signals to obtain the information signal.

15. System according to claim 14, wherein said regenerating means (19,21,22,24) generates a noise signal and comprises means (22,24) for processing said noise signal to

obtain the descrambling signal.

16. System according to claim 15, wherein said regenerating means (19,21,22,24) comprises a white noise generator (21) and filtering means (22) to obtain noise having an entropy distribution corresponding with the entropy distribution of the information signal.

17. System according to claim 15, wherein said regenerating means (19,21,22,24) comprises a narrow band noise signal generator and modulating means for modulating the narrow band noise signal to obtain noise having an entropy distribution corresponding with the entropy distribution of the information signal.

18. System according to claim 16 or 17, wherein the noise generator (21) is a pseudo random noise generator seeded by a key received from the scrambling system (1).

19. System according to any one of claims 15-18, comprising means (19) for controlling said means (22,24) for processing said noise signal, wherein said controlling means (19) receives the scrambling control information and said processing means (22,24) is controlled in accordance with said scrambling control information to provide the descrambling signal.

20. System according to any one of claims 14-19, wherein the scrambled information signal is compressed and decompressed, wherein the regenerating means (19,21,22,24) comprises means (24) for equalising the descrambling signal to compensate for compressing and decompressing of the original scrambling signal contained in the scrambled information signal.

21. System according to claim 20, wherein the equalising means (24) is adjustable by said controlling means (19), said controlling means being adapted to measure the impulse response of the compressing and decompressing operations and to adjust the equalising means to provide a corresponding impulse response.

22. System according to any one of claims 14-21, wherein at least a part of the regenerating means (19,21,22,24), in particular the noise signal generator

(21), is accommodated in a secure device (20), for example a smart card.

23. System according to claim 22, wherein the secure device (20) is adapted to add a watermark signal to the descrambling signal.

24. System according to claim 22 or 23, wherein the secure device (20) is adapted to add a compression hindering signal to the descrambling signal.

25. System according to any one of claims 14-24, wherein the scrambled information signal and the descrambling signal are digital signals, wherein means are provided for converting the scrambled signal and the descrambling signal into analogue signals, wherein the combining means (16) combine the analogue signals to obtain a clear analogue information signal.

26. System according to claim 12 for scrambling audio signals, comprising a first plurality of first narrow band filters (26), each filter having an input receiving the audio signal and an output signalling the audio signal strength in the corresponding bandwidth, a processor (6) receiving the output signals of the narrow band filters to analyse the entropy distribution of the audio signal, said processor providing the scrambling control information, a pseudo random signal generator (5) having an output, a second plurality of second narrow band filters (27) corresponding to the first plurality of first narrow band filters (26), each second filter having an input connected to the output of the random signal generator (5) and an enable and gain control input, said processor (6) being connected to the enable and gain control inputs of the second filters, wherein the output signals of the second filters are combined to obtain a noise signal having an entropy distribution corresponding with the entropy distribution of the audio signal, and wherein the noise signal is combined with the audio signal to obtain a scrambled audio signal.

27. System according to any one of claims 19-25 for descrambling a scrambled audio signal provided by the scrambling system of claim 26, wherein said processing means

(22,24) comprises a third plurality of narrow band filters (29), each filter having an input receiving the noise signal, an input receiving enable and gain control signals provided by the controlling means (19) in accordance with the scrambling control information, and an output, wherein the outputs of the filters are combined to provide the descrambling signal.

28. System according to claim 12 for scrambling still images, wherein the image information is divided in blocks and each block is transformed to obtain a set of coefficient, wherein the analysing means (3,6) analyses the entropy distribution of the transformed image information and provides the scrambling control information, wherein the generating means (5,6,7) generates noise in a two dimensional space and wherein the processing means (7) provides a filtered noise signal as scrambling signal.

29. System according to claim 28 for scrambling video, wherein a reference frame is processed as a still image, wherein next frames are compressed by determining differences with a reference frame and transforming the differences, wherein the scrambling signal used in the reference frame is reused in the next frames and wherein preferably the transformed difference signals are scrambled with a suitably processed scrambling signal.

30. System according to any one of claims 14-25 for descrambling video compressed by the system of claim 29, wherein said controlling means (19) controls the means (21,22,24) for regenerating the scrambling signal to reuse the regenerated scrambling signal for descrambling video frames which have been compressed by compressing differences with a reference frame.

31. Application of a system according to anyone of claims 11-20 for distribution of information, for example audio and/or video signals, comprising a central server (32-35,38) including means (34) for providing a key and entitlement file, means (33) for providing scrambled compressed information, and means (32) to transfer scrambled compressed information and a corresponding key and entitlement file to

one or more receiving systems (31,36) adapted to request such a transfer, each of said receiving systems having a secure device (20) receiving the key and entitlement file and providing an output used in descrambling the received scrambled compressed information.

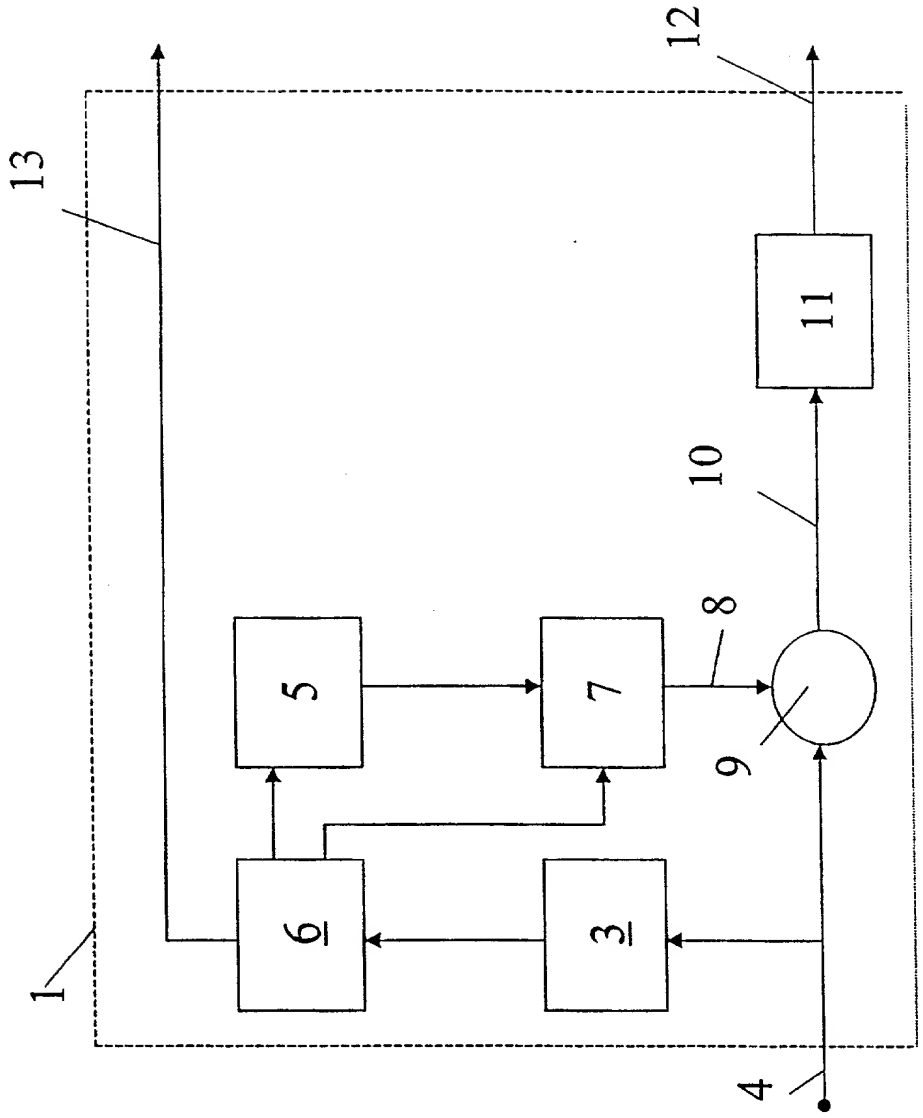

fig. 1A

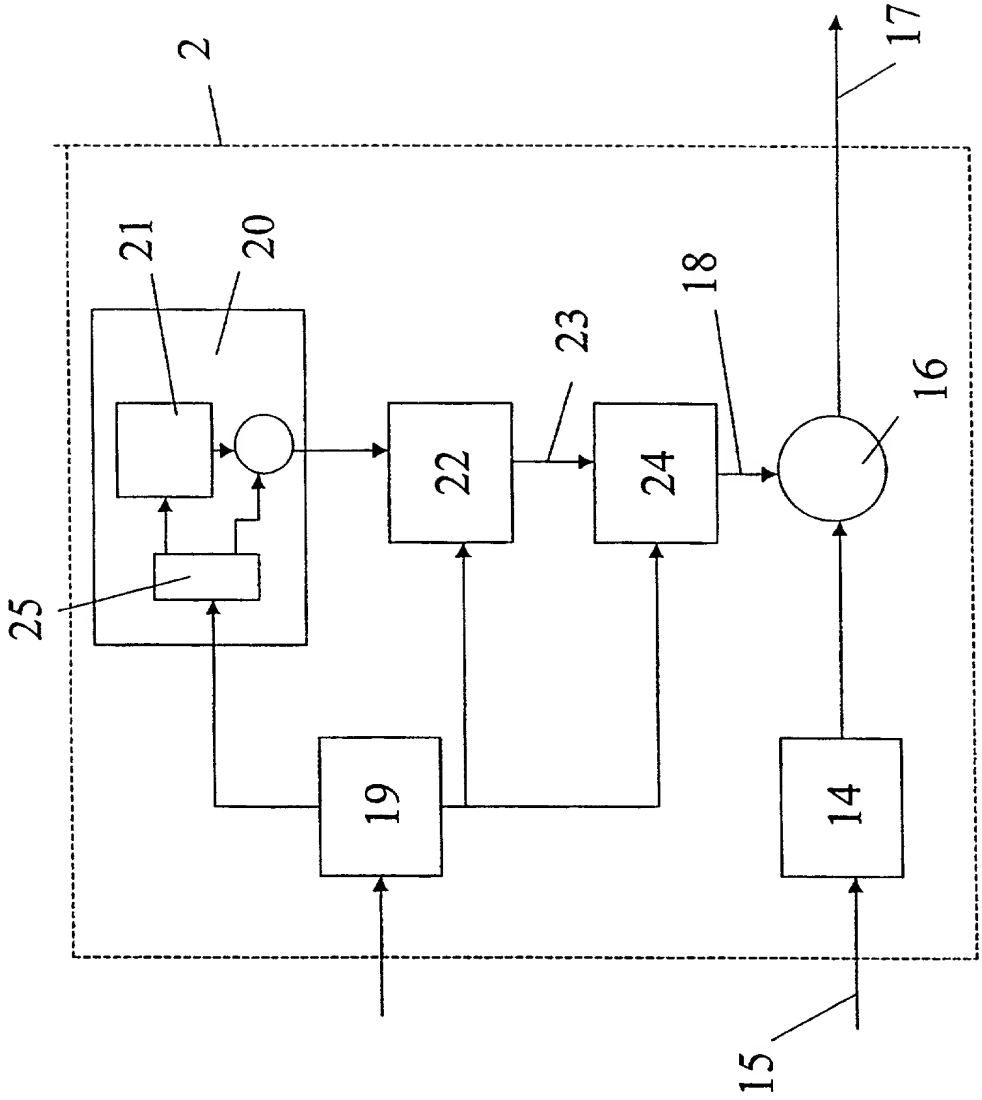

Fig 1B

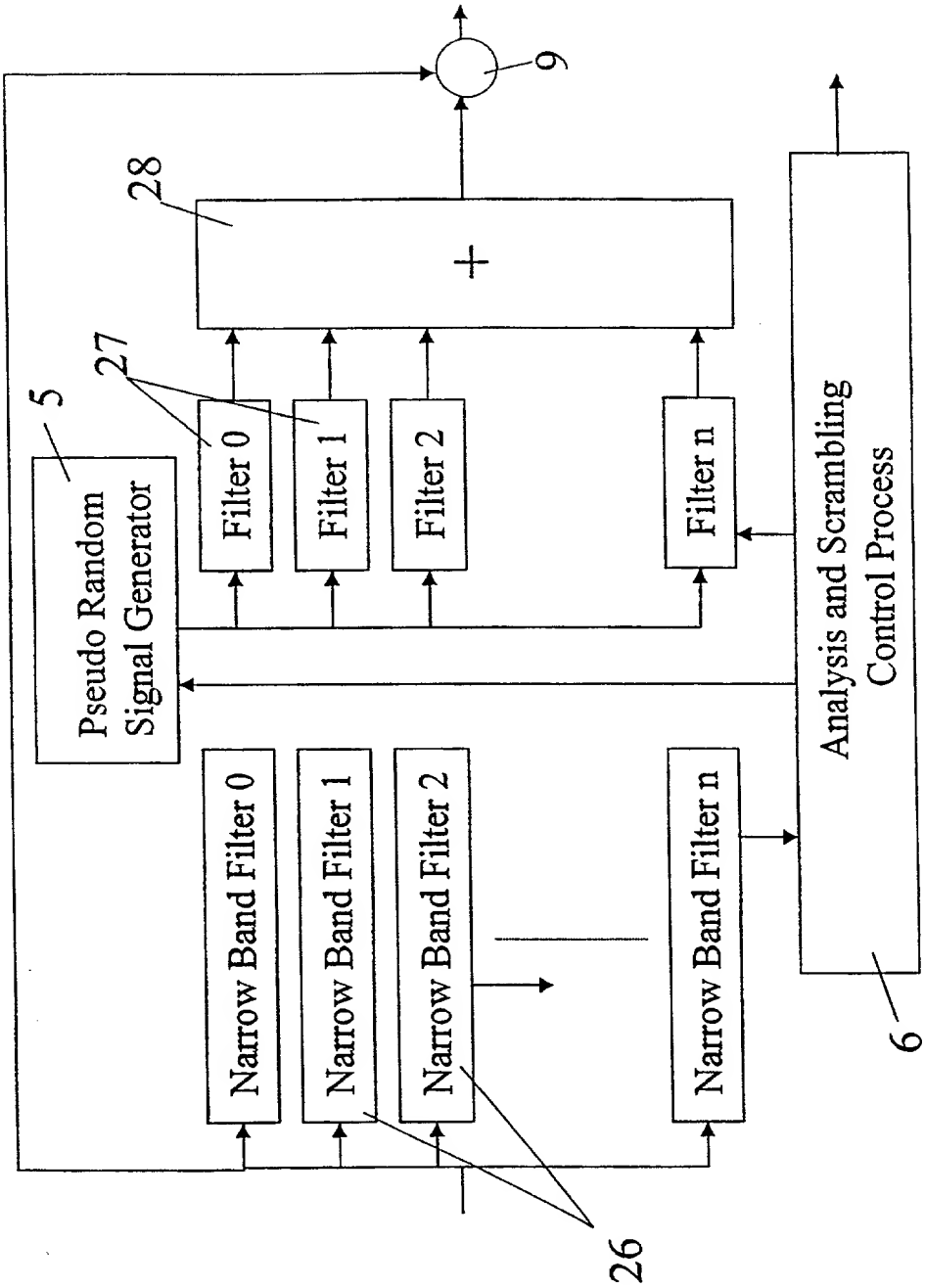
9
28
+
27
5
Pseudo Random
Signal Generator
Filter 0
Filter 1
Filter 2
Filter n
Analysis and Scrambling
Control Process
Narrow Band Filter 0
Narrow Band Filter 1
Narrow Band Filter 2
Narrow Band Filter n
26
6

Fig. 2A

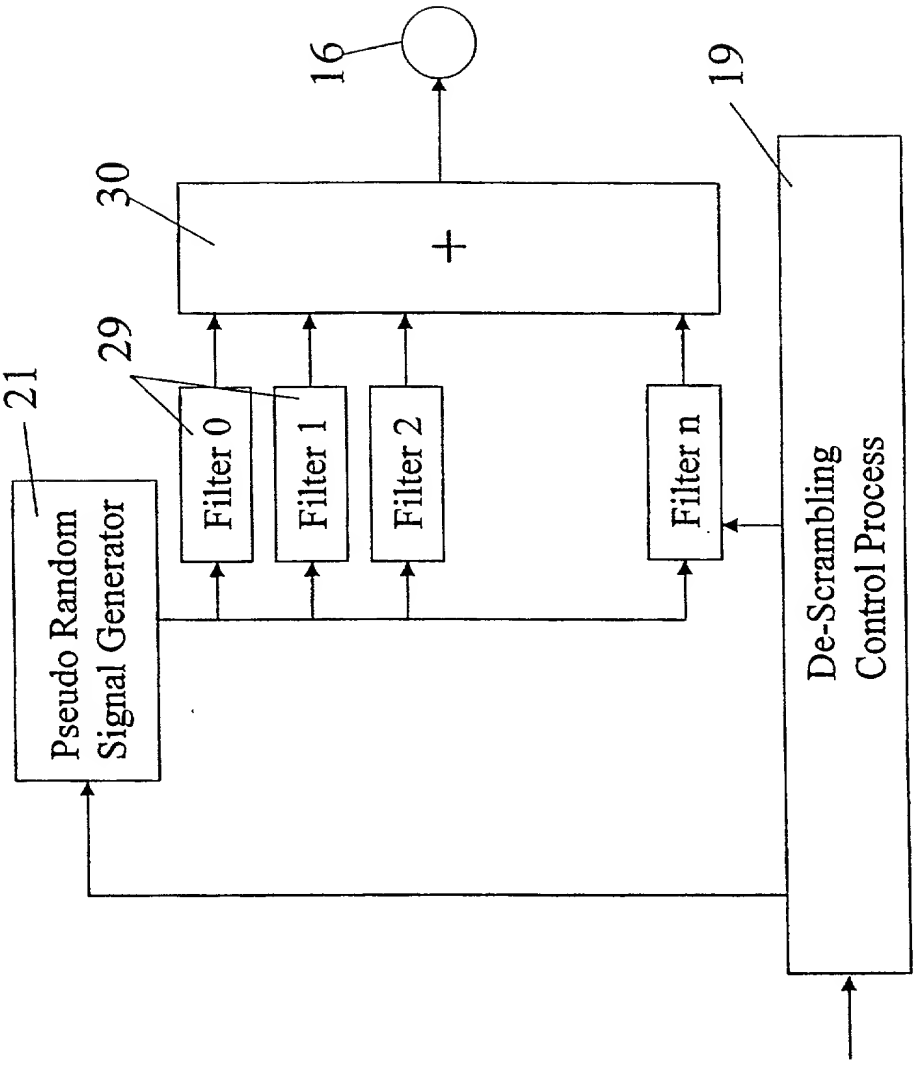
16
19
30
+
29
21
Filter 0
Filter 1
Filter 2
Filter n
Pseudo Random
Signal Generator
De-Scrambling
Control Process

fig. 2 B

20
31
Billing System
35
Key & Entitle ment Server
34
Video File Server
36
32
Internet

Fig. 3

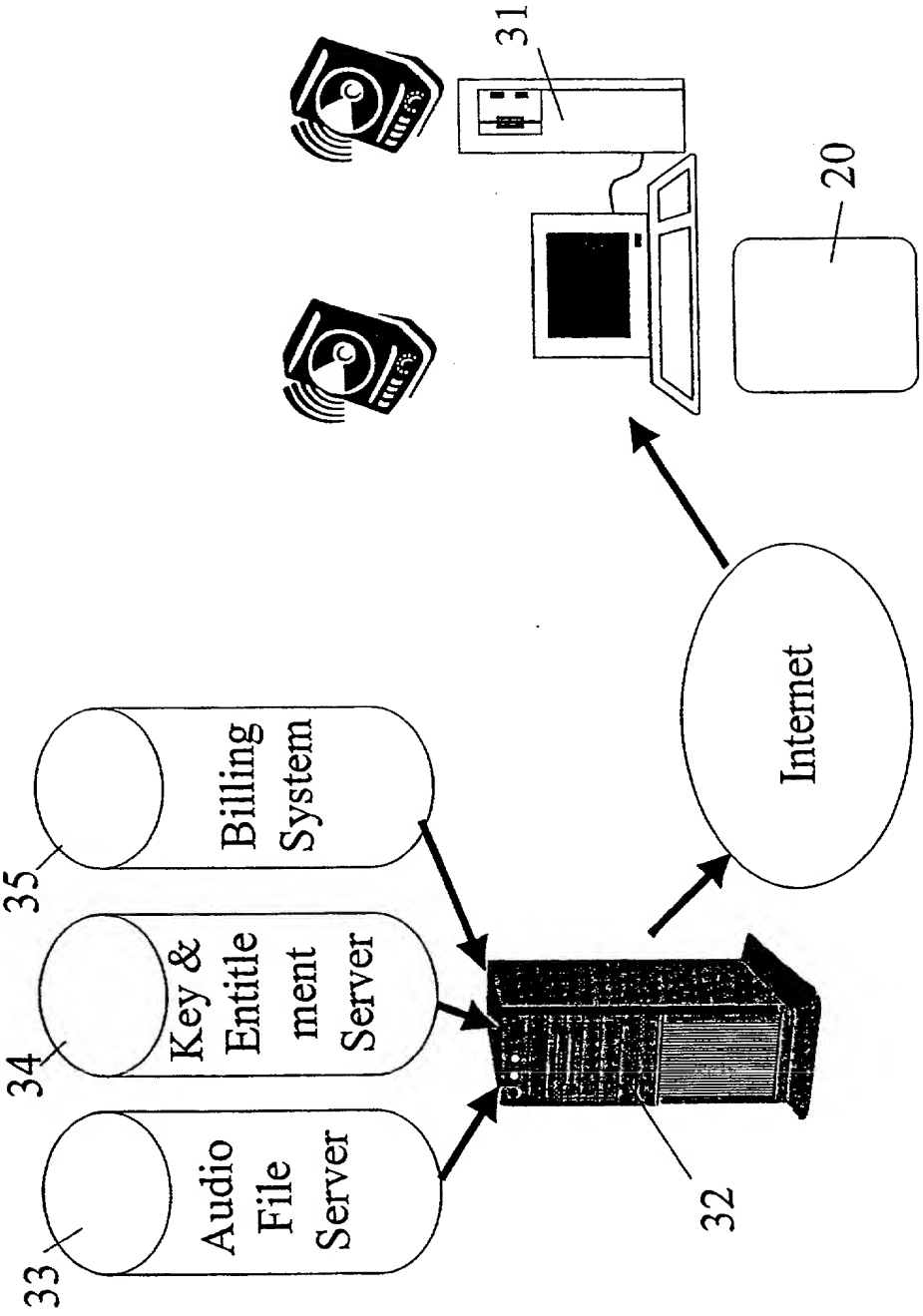
31
20
Internet
Billing System
35
Key & Entitle ment Server
34
Audio File Server
33
32

Fig. 4

09/601233
PCT/EP99/09575

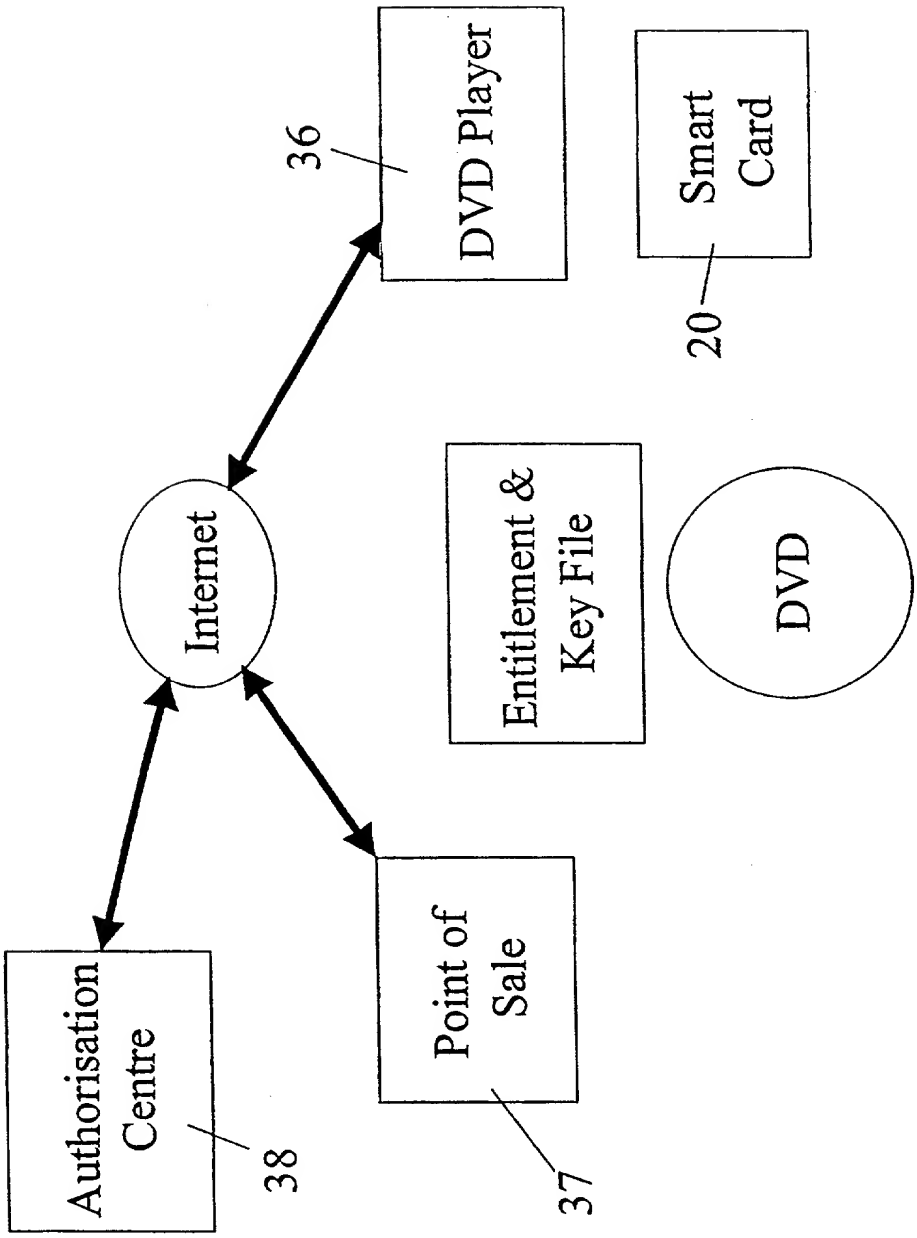

Fig. 5

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	)	
	)	
Andrew A. WAJS et al.	)	371 of International Application
	)	
Serial No.: **not yet assigned**	)	IA #: **PCT/EP99/09575**
	)	
Filed: **even date herewith**	)	IA Date: **07 December 99**
	)	
Title: **SYSTEM FOR PROCESSING AN INFORMATION SIGNAL**	)	ATTY DKT NO.: **82032-00002**

ASSOCIATE POWER OF ATTORNEY

Commisioner of Patents and Trademarks
Washington, D.C.

Sir:

The Attorney of Record, Celine Jimenez Crowson, Registration No. 40,357, hereby appoints the following registered practitioners as associate attorneys to prosecute the above-referenced application:

Matthew T. Bailey	Reg. No. 33,829
Kevin G. Shaw	Reg. No. 43,110
Ajit J. Vaidya	Reg. No. 43,214
Matthew G. Dyor	Reg. No. 45,278

Respectfully submitted,

Celine Jimenez Crowson
Attorney for Applicant
Registration No. 40,357
Hogan & Hartson, LLP
555 13th Street, N.W., Suite 701-W
Washington, D.C. 20004
PH: 202-637-5600

HOGAN & HARTSON
L.L.P.
COLUMBIA SQUARE
555 THIRTEENTH STREET NW
WASHINGTON DC 20004-1109
(202) 637-5600

Docket No. 82032-00002

Declaration and Power of Attorney for Patent Application

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name,

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought, on the invention entitled SYSTEM FOR PROCESSING AN INFORMATION SIGNAL, the specification of which was filed as International Application No. PCT/EP99/09575, filed December 7, 1999, Attorney Docket No. 82032-00002.

☐ I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

☐ I acknowledge the duty to disclose information which is material to patentability in accordance with Title 37, Code of Federal Regulations, § 1.56(a).

☐ I hereby claim foreign priority benefits under Title 35, United States Code, § 119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s)

			Priority Claimed	
98204137.8	Europe	8 December 98	[x]	[ ]
(Number)	(Country)	(Day/Month/Year)	Yes	No

Prior Foreign Application(s)

			Priority Claimed	
			[ ]	[ ]
(Number)	(Country)	(Day/Month/Year)	Yes	No

I hereby claim the benefit under Title 35, United States Code § 119(e) of any United States provisional application(s) listed below.

(Application Serial No.)	(Filing Date)

I hereby claim the benefit under Title 35, United States Code, § 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, § 112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, 1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

(Application Serial No.)	(Filing Date)	(Status)
PCT/EP99/09575	7 December 1999	

(Application Serial No.)	(Filing Date)	(Status)

I or we hereby appoint the following attorneys to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith, and request that all correspondence about the application be addressed to HOGAN & HARTSON, L.L.P., 555 13th Street, N.W., Washington, D.C. 20004

Celine Jimenez Crowson, Reg. No. 40,357

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patent issuing thereon.

FIRST NAMED INVENTOR	SIGNATURE	DATE
Andrew Augustine Wajs		22-6'00
RESIDENCE		CITIZENSHIP
NL-2023 AA Haarlem		Great Britain
POST OFFICE ADDRESS		
Schotersingel 93, NL-2023 AA Haarlem, The Netherlands		
SECOND NAMED INVENTOR	SIGNATURE	DATE
Gerard Johan Dekker		22-6'00
RESIDENCE		CITIZENSHIP
EN V LOEVESTEIN 30, NL-2151 EB NIEUW-VENNEP ~~Emmastraat 19, NL-2351 HA Leiderdorp~~		The Netherlands
POST OFFICE ADDRESS		
EN V LOEVESTEIN 30, NL-2151 EB NIEUW-VENNEP, THE NETHERLANDS ~~Emmastraat 19, NL-2351 HA Leiderdorp, The Netherlands~~		